

AMENDMENTS TO CLAIMS

This listing of claims replaces all prior versions and listings of claims:

1. (Currently Amended) An information storage medium (ISM) storing comprising means storing;

an encrypted content;

encryption key information needed in a process of decoding the encrypted content;

an information storage medium ID associated ISM ID, said associated ISM ID being which is an identifier uniquely assigned to the information storage medium; ISM; and

an information storage medium ID revocation a first list which is a list of information storage medium IDs determined as fraudulent; identifying revoked ISM ID's, said first list having an associated first version date and an associated tampering check value for checking whether said first list is untampered,

wherein,

the ISM is adapted for operation with an information processing apparatus, said apparatus having

means for executing a process for playing back content stored on the ISM,

a memory for storing a second list identifying revoked ISM ID's, said second list having an associated second version date,

means for checking whether the associated ISM ID is identical to a revoked ISM ID identified in said second list,

means for disabling the process for playing back content when the associated ISM ID is identical to a revoked ISM ID identified in said second list,

means for checking the associated tampering check value to determine whether the first

list identifying revoked ISM ID's is untampered, and

means for updating said memory, by replacing said second list with the first list, said means for updating said memory enabled to only operate when the first list is untampered and the associated first version date is later than said associated second version date.

2. (Cancelled).

3. (Currently Amended) ~~An~~ The information storage medium according to claim 1, wherein the encryption key information includes an enabling key block (EKB) as encryption key data from which a key used to decrypt the encrypted content is extractable.

4. (Currently Amended) ~~An~~ The information storage medium according to claim 3, wherein the enabling key block (EKB) is encryption key information that can be decrypted based on a device node key (DNK) provided in the form of a hierarchical key-distribution tree structure to an information processing apparatus that is a device using the information storage medium.

5. (Currently Amended) An information processing apparatus ~~for playing back a content stored on an information storage medium;~~ comprising:

means for executing a process for playing back content stored on an information storage medium (ISM), wherein both an associated ISM ID and a first list identifying revoked ISM ID's are stored on said ISM, said first list having an associated first version date;

~~a memory in which an information storage medium ID revocation list, which is a for storing a second list of information storage medium IDs determined as fraudulent, is stored; identifying revoked ISM IDs, said second list having an associated second version date;~~

~~wherein a check is made as to means for checking whether an information storage medium the associated ISM ID stored on the information storage medium is identical to one of a revoked information storage medium IDs described ISM ID identified in the storage medium information ID revocation second list stored in the memory, and, list;~~

~~if means for disabling the process for playing back content when the information storage medium~~

associated ISM ID stored on the information storage medium is not identical to any one of the a revoked information storage medium IDs described in the information storage medium ID revocation ISM ID identified in the second list, a content playback process is performed. list;

means for performing a tampering check process to check whether the first list identifying revoked ISM IDs is untampered; and

means for updating the memory, by replacing the second list with the first list, said means enabled to only operate when both: the tampering check process determines that the first list is untampered; and, the associated first version date is later than the associated second version date.

6. (Cancelled)

7. (Currently Amended) ~~An~~ The information processing apparatus according to claim 5, wherein: the information processing apparatus has a device node key (DNK) as key information provided in the form of a hierarchical key-distribution tree structure; and a key used to decrypt an encrypted content stored on the information storage medium is extracted by decoding, based on the device node key (DNK), an enabling key block (EKB) stored as encryption key information on the information storage medium.

8. (Currently Amended) An information storage medium (ISM) production ~~apparatus system comprising:~~ that produces an information storage medium such that: means for producing a plurality of ISMs and storing information on at least one ISM, said information is stored on the information storage medium, the information including comprising:

an encrypted content, encryption key information needed in a process of decoding the encrypted content, and an information storage medium ID revocation a first list which is a list of information storage medium IDs determined as fraudulent; identifying revoked ISM ID's, said first list having an associated first version date and an associated tampering check value for checking whether the first list is untampered, and an information storage medium associated ISM ID, which is said associated ISM ID being an identifier uniquely assigned to each information storage medium, is stored on each produced information storage medium such that each information storage medium has a different information storage medium ID ISM;

wherein, the at least one ISM is adapted for operation with an information processing apparatus, said apparatus having:

means for executing a process for playing back content stored on the ISM;

a memory for storing a second list identifying revoked ISM ID's, said second list having an associated second version date;

means for checking whether the associated ISM ID is identical to a revoked ISM ID identified in the second list;

means for disabling the process for playing back content when the associated ISM ID is identical to a revoked ISM ID identified in the second list;

means for checking the associated tampering check value to determine whether the first list identifying revoked ISM ID's is untampered; and

means for updating the memory, by replacing the second list with the first list, said means for updating the memory enabled to only operate when the first list is untampered and the associated first version date is later than the associated second version date.

9. (Cancelled)

10. (Currently Amended) ~~An~~ The information storage medium production apparatus according to claim 8, wherein the encryption key information includes an enabling key block (EKB) as encryption key data to be applied in the decryption of the encrypted content.

11. (Currently Amended) An information processing method of ~~playing back content stored on an information storage medium~~ comprising the steps of:

executing, with an information processing apparatus, a process for playing back content stored on an information storage medium (ISM), wherein both an associated ISM ID and a first list identifying revoked ISM ID's are stored on said ISM, said first list having an associated first version date, said executing step further comprising:

reading information storage medium ID stored on the information storage medium; the associated ISM ID;

checking whether the information storage medium associated ISM ID stored on the information storage medium is identical to one of a revoked information storage medium IDs ISM ID described identified in a storage medium information ID revocation list, which is a second list of invalid information storage medium IDs and which is identifying revoked ISM ID's, said second list having an associated second version date, and said second list being stored in a memory of ~~an~~ the information processing apparatus; and

playing back disabling the process for playing back content if and only if when the information storage medium associated ISM ID stored on the information storage medium is not identical to any one of the a revoked information storage medium IDs described in the information storage medium ID revocation list, ISM ID identified in the second list;

performing a tampering check process to check whether the first list identifying revoked ISM ID's is untampered; and

updating the memory of the information processing apparatus, by replacing the second list with the first list, only when both: the tampering check process determines that the first list is untampered; and, the associated first version date is later than the associated second version date.

12. (Cancelled)

13. (Currently Amended) ~~An~~ The information processing method according to claim 11, further comprising the step of acquiring a key used to decode an encrypted content stored on the information storage medium by decoding an enabling key block (EKB) stored as encryption key information on the information storage medium, the decoding of the enabling key block (EKB) being based on a device node key (DNK) provided as key information provided in the form of a hierarchical key-distribution tree structure.

14. A method of producing an An information storage medium (ISM) production method, comprising the step of:

storing, on the producing a plurality of ISMs and storing information on at least one ISM, said information storage medium, comprising:

an encrypted content, encryption key information needed in a process of decoding the encrypted content, and an information storage medium ID revocation a first list which is a list of information storage medium IDs determined as fraudulent; identifying revoked ISM ID's said first list having an associated first version date and storing an information storage medium ID, which is an associated tampering check value for checking whether the first list is untampered, and an associated ISM ID, said associated ISM ID being an identifier uniquely assigned to each information storage medium, on each produced information storage medium such that each information storage medium has a different information storage medium ID ISM;

wherein, the at least one ISM is adapted for operation with an information processing apparatus, said apparatus having:

means for executing a process for playing back content stored on the ISM;

a memory for storing a second list identifying revoked ISM ID's, said second list having an associated second version date;

means for checking whether the associated ISM ID is identical to a revoked ISM ID identified in the second list;

means for disabling the process for playing back content when the associated ISM ID is identical to a revoked ISM ID identified in the second list;

means for checking the associated tampering check value to determine whether the first list identifying revoked ISM ID's is untampered; and

means for updating the memory, by replacing the second list with the first list, said means for updating the memory enabled to only operate when the first list is untampered and the associated first version date is later than the associated second version date.

15. (Currently Amended) A computer program that executes readable medium encoded with a computer

program for executing a process of for playing back a content stored on an information storage medium (ISM), wherein both an associated ISM ID and a first list identifying revoked ISM ID's are stored on said ISM, said first list having an associated first version date, said process comprising the steps of:

reading information storage medium ID stored on the information storage medium; the associated ISM ID;

checking whether the information storage medium associated ISM ID stored on the information storage medium is identical to one of a revoked information storage medium IDs, ISM ID described identified in a storage medium information ID revocation list, which is a second list of invalid information storage medium IDs and which is identifying revoked ISM ID's, said second list having an associated second version date, and said second list being stored in a memory of on the information processing apparatus; and

playing back disabling the process for playing back content if and only if when the information storage medium associated ISM ID stored on the information storage medium is not identical to any one of the a revoked information storage medium IDs described in the information storage medium ID revocation list, ISM ID identified in the second list;

performing a tampering check process to check whether the first list identifying revoked ISM ID's is untampered; and

updating the memory of the information processing apparatus, by replacing the second list with the first list, only when both: the tampering check process determines that the first list is untampered; and, the associated first version date is later than the associated second version date.